Activity: **5.5**
                      Design System Security Controls

Responsibility: Project Team Analysts and Security Personnel

Description: Design the security controls that will be incorporated into the software product based on the security and access requirements identified during the Requirements Definition Stage. Design the security controls in conjunction with the site or system owner organization's Computer System Security Officer (CSSO) or the Assistant Computer Protection Program Manager (ACPPM).

Procedure: Use the following procedure to implement the design process.

- Identify the users and organizations that will have access to the software product. Indicate what access restrictions they will have. All persons in a work area may not have the same security access level. Measures should be taken to assure that sensitive materials and software requiring protection are not accessed by unauthorized individuals.

- Identify controls for the software product, such as the user identification code for system access and the network access code for the network on which the software product will reside.

- Identify whether access restrictions will be applied at the system, subsystem, transaction, record, or data element levels. Classified information must be protected in accordance with DOE directives.

- Identify physical safeguards required to protect hardware, software, or information from natural hazards and malicious acts.

- Identify communications security requirements.

Work Product: Document the design for the system security controls in accordance with the project design standards. Discuss the design with the system owner and users and submit the completed design for their review and approval. The approved design will be incorporated into the Functional Design Document. Place a copy of the system security control design in the Project File.

Review Process: Schedule a structured walkthrough to verify that the system security controls are correct and complete. Include the CSSO or the ACPPM in the walkthrough.

References: •   DOE 5639.6, CLASSIFIED COMPUTER SECURITY PROGRAM, September 15, 1992.

•   DOE HEADQUARTERS UNCLASSIFIED COMPUTER PROTECTION PLAN, February 1995.